REMARKS

1. Before discussing all objections raised in the Office Action in detail, Applicant will summarize the key features of the invention as defined by the amended claims.

Basically, the invention generate's a second data stream from a first data stream including a first header and a first payload data block so that, when considering the scenario of Fig. 4, a receiver that, in the embodiment, receives a data stream bound to his PC can decrypt it and re-encrypt it for his other devices, such as car hifi, home hifi, or solid state player, to get a second data stream from a first data stream.

According to the newly submitted Claim 1, the data stream supplied by the supplier for multi-media data, designated 102 in Fig. 4, includes, in the first header, a supplier identification specifying the supplier 102, and a user identification specifying the user-PC 104, *i.e.* the destination of the data stream. The receiver-PC inserts the information from the first header, *i.e.* supplier identification for the supplier 102 and user identification for the receiver-PC 104, as information allowing conclusions regarding the origin of the payload data, into the new second data stream. The receiver-PC that, for example, carries out the method defined in Claim 1 further enters current supplier information into the second header, *i.e.* it enters itself as supplier and, for example, the car hifi system 106a as user identification, *i.e.* as destination of the second data stream. Thus, a second data stream contains an unbroken chain of supplier identifications and user identifications, wherein this unbroken chain further comprises redundancy in that the user identification in the first header, *i.e.* the identification for the receiver-PC 104 of Fig. 4, has to match the supplier identification of the second header, wherein the supplier of the second data stream, i.e. the supplier identification in the second header, is also the receiver-PC 104.

According to the invention, this redundancy is used by a method for playing according to Claim 15 and/or by an apparatus for playing according to Claim 21 to perform a verification of the origin of the second data stream based on this redundancy, wherein this second data stream is only played by a legalized player if this legalized player finds that the second supplier identification matches the first user identification (positive result of the verification). If the

verification provides a negative result, however, the playing of the second data stream is refused.

The inventive concept consists, on the one hand, of generating a second data stream from a first data stream with redundant and unbroken origin information chain of user identification and supplier identification, and consists, on the other hand, of a method and an apparatus for playing the second data stream, wherein the redundancy in the origin information chain of user identification and supplier identification is used to play only data streams whose origin is documented in an unbroken way, and allows an efficient security measure which may be implemented with little calculating effort in every respect to prevent the illegal manipulating/copying and, generally speaking, stealing of intellectual property for legalized players.

The inventive concept is easy to implement and, particularly with respect to market acceptance and market feasibility, may be implemented without a central authority or the like.

2. In the following, the original disclosure is shown for the newly submitted claims. The modifications in the first paragraph of the newly submitted Claim 1 are based on Fig. 3, element 28 and/or elements 42 and 44, wherein 42 represents the supplier identification and 44 represents the user identification. Furthermore, see the second paragraph on page 14 of the description.

The modifications in the third paragraph of the newly submitted Claim 1 are also based on Fig. 3 and on page 23, first four lines.

In addition, see the originally filed Claim 2 and the originally filed Claim 4. Additional support is also provided by the originally filed Claim 8.

The modifications in the fourth paragraph of Claim 1 are also based on the originally filed Claims 2 and 4 and on the second paragraph of page 21 of the description, namely lines 7-9 thereof.

The newly submitted Claim 15 is based on the first complete paragraph on page 26 of the description, particularly on the second paragraph on page 26 of the description. In addition, see Fig. 7, block 138, with respect to supporting the last paragraph of the newly submitted claim 15.

The newly submitted Claim 19 is based on the originally filed Claim 19 and on the same original disclosure as referred to in connection with Claim 1.

The newly submitted Claim 21 is based on the same original disclosure as referred to for the newly submitted Claim 15.

3. Applicant now discusses the objections raised in the Office Action.

The formal claim objections under section 1 of the Office Action have been accounted for in the amended claims.

Regarding the objections against the specification, please see the enclosed replacement pages.

4. Under section 2 of the Office Action, the Examiner objects to most of the claims as directed to non-statutory subject matter. However, Claim 1 does not define the conversion of one set of numbers to another set of numbers. Instead, the method receives, as an input, a first data stream having a first header and a first payload data block with payload data, and outputs a second data stream. Because data streams are technical items, this objection is not justified. Additionally, amended Claim 1 further defines that the first header comprises a first supplier identification for a supplier of the first data stream and the first user identification for a receiver of the first data stream. The supplier identification as well as the user identification may, of course, be represented by binary numbers. However, these binary numbers have a specific meaning, *i.e.* they point to certain entities generating or using a data stream. The same applies to the steps of extracting, generating, entering, and generating.

To confine the subject matter invention to a statutory class, Applicant has added the following limitation to the last paragraph of claim 1:

"wherein the payload data include audio data, video data, a combination of audio data and video data, or text data".

This amendment is supported by the paragraph bridging pages 5 and 6 of the final version to be filed as preliminary amendment as enclosed with my other letter.

Finally, Applicant has amended the method claims to indicate that the steps recited therein are "computer implemented."

Regarding Claim 5, please refer to amended claim 5.

Regarding the Examiner's objection against Claim 19 as directed to non-statutory subject matter, the same arguments as outlined with respect to Claim 1 apply.

5. With regard to section 10 of the Office Action:

Cannella discloses a data transmission protocol method and apparatus for mapping received data into a payload field of a packet, for counting bytes mapped into the payload field, and for generating first and second headers, the first and second headers preceding the payload field of an output data packet as defined in column 2, lines 61 to 64. Furthermore, as shown in Fig. 3, a CRC (cyclic redundancy check) field is appended to the payload field. As disclosed in column 10, lines 11 to 19, the CRC field contains the result of performing a cyclic redundancy check across the byte count field and the payload field. To this end, a CRC-CCITT polynomial is used for this calculation. Enclosed with this response are pages from the well-known Handbook of Applied Cryptography. Particularly, please refer to page 363, where a CRC or cyclic redundancy code is discussed in general. In the fifth line of section 9.80, such a polynomial for calculating a CRC is illustrated.

Importantly, note that a CRC algorithm simply maps arbitrary length inputs into k-bit imprints. Stated differently, the CRC in Cannella is calculated only based on the data in the payload field and the byte count (BC) field. No additional information is necessary or is used for calculating the CRC field data.

When the Fig. 3 data are considered as the second data stream as defined in the first line of Claim 1, then Canella does not disclose a first data stream having a first payload data block and a first header. Instead, column 2, line 61 simply mentions "received data" without saying that these data include payload data and a header.

Furthermore, Canella does not disclose that the first header comprises a first supplier identification for a supplier of the first data stream and a first user

identification for a receiver of the first data stream. Instead, column 2, line 61 simply mentions "received data" without giving any details on these received data.

Therefore, Canella also does not disclose the step of extracting, because the received data are not disclosed to have a header. The Examiner's statement that a single data packet anticipates the first data stream and the second data stream is not correct logic. How could a single packet be identical to two data streams?

Canella also does not disclose the step of generating a second header for the second data stream, wherein the second header comprises a second supplier identification for a supplier of the second data stream and a second user identification for a receiver of the second data stream. When one considers the SSC data field or the byte count field of Fig. 3 as the "second header" of Claim 1, then it becomes clear that neither the SSC nor the BC include a second supplier identification for a supplier of the second data stream and a second user identification for a receiver of the second data stream.

Canella also does not disclose the step of entering at least a part of the first header into the second header, wherein the part of the first header includes information, wherein this information comprises the first supplier identification for the supplier of the first data stream and the first user identification for the receiver of the first data stream. Because Canella does not disclose the specific definition of the first header (indeed, Canella does not disclose a first header at all, as discussed above), Canella can also not disclose that this first header is entered into the second header. The Examiner takes the position that the CRC field is comparable to the part of the first header, which is entered into the second header. However, the Examiner's arguments are contradictionary, because the Examiner stated that SSC field or BC field are the second header and then says that the CRC field is introduced into the second header, although the CRC field is written behind the payload data in Canella, *i.e.*, separate from the SSC or BC fields. The Examiner is incorrect when stating that a CRC requires information of the origin of the data as outlined in the second paragraph of page 5 of the Office Action. While the Examiner is correct when stating that a CRC is used for error detection (this is also stated on page 363 of the Handbook of Applied Cryptography), it is incorrect to state that a CRC

requires information on the origin of the data. The Examiner asserts this without giving any support for this assertion.

Therefore, the Examiner's objections against originally filed Claim 2 are also not justified because a CRC does not include information of the origin of the data, which identifies the sender of the data packet, so that the receiver can detect errors. Note that for detecting errors, the sender of a data packet is not required. Only the data itself are required. A CRC does not use any information of the origin of the data, but only uses information on the data itself, which is also completely in line with page 363 of the well-known Handbook of Applied Cryptography.

6. Applicant now discusses the Examiner's objections against Claim 8. The features of originally filed Claim 8 are now included in Claim 1. This also applies for the features of originally filed Claim 2.

As outlined in the penultimate paragraph of page 8, the Examiner is incorrect when stating that Cannella teaches a second header with a receiver identification as a user identification. This is due to the fact that a CRC does not require any information on the origin of the data, but only requires the data itself.

In the first paragraph of page 9, the Examiner states that Erickson teaches entering an identification of the receiver of the first data stream as user identification into a part of the second header. However, amended Claim 1 states that the second user identification is a receiver of the second data stream, rather than a receiver of the first data stream which is, of course, part of the first header rather than the second header.

Thus, in accordance with the invention, the second header includes, when the steps of Claim 1 have been performed, information on the supplier of the first data stream and a first user identification for a receiver of the first data stream as part of the first header and, also includes an identification for a supplier of the second data stream and an identification of the receiver of the second data stream. Erickson only retains original and derivative authors to retain a copyright "family tree" as stated in column 3, lines 55 to 58, so that any modifications to a document can be associated with entities performing these modifications. However, Erickson does not include any information on an

intended user receiver of the first data stream or the second data stream. When Erickson is compared to claim 1, then this "family tree" or electronic bibliographic record mentioned in column 3, line 57, does not include a first user identification for a receiver of the first data stream and does not include a second user identification for a receiver of the second data stream.

Therefore, also a combination of documents Erickson and Canella will not result in the inventive claims. Thus, the prior art documents alone or in combination do not disclose a method, which provides an unbroken chain of supplier identifications and user identifications, wherein this unbroken chain further comprises redundancy in that the user identification in the first header has to match the supplier identification of the second header, wherein the supplier of the second data stream, *i.e.*, the supplier identification in the second header, is also the receiver of the first data stream, when everything went well. When, however, there was any fraud or non-allowed manipulation, then the second supplier identification is not identical to the first user identification so that, as defined in amended Claim 15, this verifying step checking identity between those items outputs a negative result, which leads to a refusal to play the second data stream.

Respectfully submitted,

Michael A. Glenn
Reg. No. 30,176

Customer No. 22,862